Конфигурация безопасности коммутатора

Топология

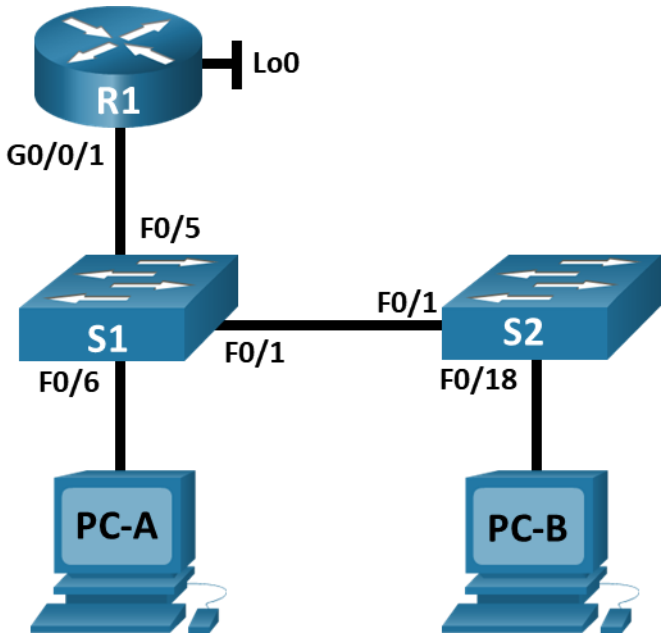

Таблица адресации

Устройство	interface/vlan	IP-адрес	Маска подсети
R1_ФАМИЛИЯ	G0/0/1	192.168.X+10.1	255.255.255.0
	Loopback 0	10.10.1.1	255.255.255.0
S1	VLAN X+10	192.168.X+10.201	255.255.255.0
S2	VLAN X+10	192.168.X+10.202	255.255.255.0
PC A	NIC	DHCP	255.255.255.0
PC B	NIC	DHCP	255.255.255.0

Цели

Часть 1. Настройка основного сетевого устройства

- Создайте сеть.
- Настройте маршрутизатор R1_ФАМИЛИЯ.
- Настройка и проверка основных параметров коммутатора

Часть 2. Настройка сетей VLAN

- Сконфигуриуйте VLAN X+10.
- Сконфигуриуйте SVI для VLAN X+10.
- Настройте VLAN 333 с именем Native на S1 и S2.
- Настройте VLAN 999 с именем ParkingLot на S1 и S2.

Часть 3: Настройки безопасности коммутатора.

- Реализация магистральных соединений 802.1Q.
- Настройка портов доступа
- Безопасность неиспользуемых портов коммутатора
- Документирование и реализация функций безопасности порта.
- Реализовать безопасность DHCP snooping .
- Реализация PortFast и BPDU Guard
- Проверка сквозной связанности.

Необходимые ресурсы

- 1 Маршрутизатор (Cisco 4221 с универсальным образом Cisco IOS XE версии 16.9.3 или аналогичным)
- 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.0(2) (образ lanbasek9) или аналогичная модель)
- 2 ПК (ОС Windows с программой эмуляции терминалов, такой как Tera Term)
- Консольные кабели для настройки устройств Cisco IOS через консольные порты.
- Кабели Ethernet, расположенные в соответствии с топологией

Инструкции

Часть 1. Настройка основного сетевого устройства

Шаг 1. Создайте сеть.

a. Создайте сеть согласно топологии.

b. Инициализация устройств

Шаг 2. Настройте маршрутизатор R1_ФАМИЛИЯ.

a. Загрузите следующий конфигурационный скрипт на R1_ФАМИЛИЯ.

```
enable
configure terminal
hostname R1_ФАМИЛИЯ
no ip domain lookup
ip dhcp excluded-address 192.168.X+10.1 192.168.X+10.9
ip dhcp excluded-address 192.168.X+10.201 192.168.X+10.202
!
ip dhcp pool Students
 network 192.168.X+10.0 255.255.255.0
```

```
 default-router 192.168.X+10.1
 domain-name CCNA2.Lab-7
!
interface Loopback0
 ip address 10.10.1.1 255.255.255.0
!
interface GigabitEthernet0/0/1
 description Link to S1
 ip dhcp relay information trusted
 ip address 192.168.X+10.1 255.255.255.0
 no shutdown
!
line con 0
 logging synchronous
 exec-timeout 0 0
```

b. Проверьте конфигурацию сетевых интерфейсов на R1_ФАМИЛИЯ.

c. Убедитесь, что IP-адресация и интерфейсы находятся в состоянии up / up (при необходимости устраните неполадки).

Шаг 3. Настройка и проверка основных параметров коммутатора

a. Настройте имя хоста для коммутаторов S1 и S2.

b. Запретите нежелательный поиск в DNS.

c. Настройте описания интерфейса для портов, которые используются в S1 и S2.

d. Установите для шлюза по умолчанию для VLAN управления значение 192.168.X+10.1 на обоих коммутаторах.

Часть 2. Настройка сетей VLAN на коммутаторах.

Шаг 1. Сконфигуриуйте VLAN X+10.

Добавьте VLAN X+10 на S1 и S2 и назовите VLAN - **Management.**

Шаг 2. Сконфигуриуйте SVI для VLAN X+10.

Настройте IP-адрес в соответствии с таблицей адресации для SVI для VLAN X+10 на S1 и S2. Включите интерфейсы SVI и предоставьте описание для интерфейса.

Шаг 3. Настройте VLAN 333 с именем Native на S1 и S2.

Шаг 4. Настройте VLAN 999 с именем ParkingLot на S1 и S2.

Часть 3. Настройки безопасности коммутатора.

Шаг 1. Релизация магистральных соединений 802.1Q.

a. Настройте все магистральные порты Fa0/1 на обоих коммутаторах для использования VLAN 333 в качестве native VLAN.

b. Убедитесь, что режим транкинга успешно настроен на всех коммутаторах с помощью команды **show interface trunk** на обоих коммутаторах.

c. Отключить согласование DTP F0/1 на S1 и S2.

d. Проверьте с помощью команды **show interfaces**. Пример:

```
S1# show interfaces f0/1 switchport | include Negotiation
Negotiation of Trunking: Off
```

Шаг 2. Настройка портов доступа

a. На S1 настройте F0/5 и F0/6 в качестве портов доступа и свяжите их с VLAN X+10.

b. На S2 настройте порт доступа Fa0/18 и свяжите его с VLAN X+10.

Шаг 3. Безопасность неиспользуемых портов коммутатора

a. На S1 и S2 переместите неиспользуемые порты из VLAN 1 в VLAN 999 и отключите неиспользуемые порты.

b. Убедитесь, что неиспользуемые порты отключены и связаны с VLAN 999, введя команду **show interfaces status**.

Шаг 4. Документирование и реализация функций безопасности порта.

Интерфейсы F0/6 на S1 и F0/18 на S2 настроены как порты доступа. На этом шаге вы также настроите безопасность портов на этих двух портах доступа.

a. На S1 введите команду **show port-security interface f0/6** для отображения настроек по умолчанию безопасности порта для интерфейса F0/6. Запишите свои ответы ниже.

Конфигурация безопасности порта по умолчанию	
Функция	**Настройка по умолчанию**
Защита портов	
Максимальное количество записей MAC-адресов	
Режим проверки на нарушение безопасности	
Aging Time	
Aging Type	
Secure Static Address Aging	
Sticky MAC Address	

b. На S1 включите защиту порта на F0/6 со следующими настройками:

- Максимальное количество записей MAC-адресов: **3**
- Режим безопасности: **restrict**
- Aging time: **60 мин.**
- Aging type: **неактивный**

c. Проверьте настройки защиты порта (**port-security**) на S1 для интерфейса F0/6. Далее просмотрите выходные данные команды **show port-security address**.

d. Включите безопасность порта для F0/18 на S2. Настройте каждый активный порт доступа таким образом, чтобы он автоматически добавлял адреса MAC, изученные на этом порту, в текущую конфигурацию.

e. Настройте следующие параметры безопасности порта на S2 F0/18:

   - Максимальное количество записей MAC-адресов: **2**
   - Тип безопасности: **Protect**
   - Aging time: **60 мин.**

f. Проверьте настройки защиты порта (**port-security**) на S2 для интерфейса F0/18. Далее просмотрите выходные данные команды **show port-security address**.

Шаг 5. Реализовать безопасность DHCP snooping.

a. На S2 включите DHCP snooping и настройте DHCP snooping во VLAN X+10.

b. Настройте магистральные порты на S2 как доверенные порты.

c. Ограничьте ненадежный порт Fa0/18 на S2 пятью DHCP-пакетами в секунду.

d. Проверьте DHCP Snooping на S2 с помощью команды **show ip dhcp snooping**.

e. В командной строке на PC-B освободите, а затем обновите IP-адрес.

```
C:\Users\Student> ipconfig /release
C:\Users\Student> ipconfig /renew
```

f. Проверьте привязку отслеживания DHCP с помощью команды **show ip dhcp snooping binding**.

Шаг 6. Реализация PortFast и BPDU Guard

a. Настройте PortFast на всех портах доступа, которые используются на обоих коммутаторах.

b. Включите защиту BPDU на портах доступа VLAN X+10 для S1 и S2, подключенных к PC-A и PC-B.

c. Убедитесь, что защита BPDU и PortFast включены на соответствующих портах с помощью команды **show spanning-tree interface f0/6 detail**.

Шаг 7. Проверьте наличие сквозного подключения.

Отправьте эхо-запрос между всеми устройствами в таблице IP-адресации.

Вопросы для защиты теоретической части (глава 11)

1. Для чего необходимо обеспечить безопасность портов коммутатора? Что произойдет, если к порту с включенной безопасностью подключают более одного устройства и почему?

2. Какое минимальное и максимальное количество MAC-адресов может быть разрешено на одном порту коммутатора? Опишите все существующие способы изучения MAC-адресов на коммутаторе.

3. Опишите существующие типы устаревания безопасности порта. Каким образом можно активировать отключенный по ошибке порт коммутатора?

4. Дайте характеристику режимам нарушения безопасности порта. В чем заключается опасность включенного протокола согласования DTP?

5. Опишите суть технологии DHCP Snooping. Для чего может понадобиться динамическая проверка ARP?

6. Перечислите рекомендации по настройке портов с помощью динамической проверки ARP. Почему необходимо включать функции BPDU Guard И PortFast?

7. Какие шаги необходимо предпринять для устранения угрозы VLAN Hopping?

8. Что рекомендуется сделать при использовании сети native VLAN? Какие два типа портов коммутаторов используются на коммутаторах Cisco в составе средств защиты от атак DHCP-спуфинга?

9. Почему устройства уровня 2 считаются самым слабым звеном в инфраструктуре безопасности компании? Где хранятся динамически определяемые MAC-адреса, когда включена функция sticky learning?